Space Shuttle Range Safety Panel

During 2007, the Space Shuttle Range Safety Panel dealt with a number of topics related to the Space Shuttle. Included were Shuttle main engine reliability assessment, advanced master events controller spurious output testing, and ceiling and visibility launch commit criteria. Also addressed were command receiver decoder implementation and public entry risk assessment flight rule updates.

Space Shuttle Main Engine Reliability Assessments

During the past several years, NASA and the 45th Space Wing have made significant progress on updating the launch area risk assessment input parameters that are used as part of the process of estimating public risk for each Shuttle launch. One of the input parameters pertains to vehicle failure probabilities and is addressed using the Shuttle probabilistic risk assessment data generated by NASA. The NASA probabilistic risk assessment data include both a failure probability estimate and a time distribution for each identified failure mode. The probability estimate and time distribution for Space Shuttle main engine related failures were reassessed in 2007. Prior NASA studies indicated that a uniform distribution (i.e., constant failure probability as a function of time in flight) was the most appropriate distribution for main engine failures.

The Space Shuttle main engine failure distribution was reanalyzed by both NASA and 45th Space Wing personnel, and the results were discussed at the Range Safety Panel in April 2007. The conclusion from that panel meeting was that the uniform distribution was the most representative distribution based on the current Space Shuttle main engine data and analyses compiled to date. As a result, the launch area risk assessment input parameters pertaining to failure time distributions remained unchanged.

Advanced Master Events Controller Spurious Output Testing

During advanced master events controller testing in the Shuttle Avionics Integration Lab, it was noted that advanced master events controller outputs would spuriously turn on when the controllers are powered down. This raised concern as to whether the spurious advanced master events controller commands could trigger the solid rocket booster range safety safe and arm device to the SAFE position and/or left or right solid rocket booster range safety Power Off (command receiver/decoder off).

Research into the anomalous advanced master events controller condition and the interface circuit design led the Range to conclude that spurious output of the solid rocket booster range safety SAFE is acceptable for all vehicles/missions. Each advanced master events controller controls 1 of 2 switches in series between the command receiver decoder and the safe and arm device. The switches are non-latching and reset within 50 milliseconds (per command receiver decoder specification) after power is removed. The worst-case circuit analysis shows they actually reset within 8.7 milliseconds.

Space Shuttle Range Safety Panel

To impact the safe and arm device, spurious output from both advanced master events controllers would need to occur within 8.7 milliseconds, which was considered non-credible. Additionally, the voltage/duration observed will not reset the switch.

Research into the anomalous advanced master events controller condition and the interface circuit design led the Range to conclude that spurious output to the solid rocket booster range safety system safe and arm is acceptable for all vehicles/missions. The maximum spurious output voltage seen on the STS-123 installed advanced master events controllers was 13.3 Vdc for 300 microseconds. Worst-case circuit analysis showed that spurious master events controller inputs to the command receiver decoder of 32 Vdc for less than 2.6 milliseconds will not latch the command receiver decoder.

Also, worst-case circuit analysis showed that spurious master events controller inputs to the command receiver decoder that are less than 14.4 Vdc (steady state) will not latch the command receiver decoder. So the maximum advanced master events controller voltage output/duration seen to date will not reset the command receiver decoders. Given this data and the understanding of the cause of the condition, the Range has accepted this condition “as is” for all flights provided that testing is done no earlier than 6 months before scheduled launch to ensure the anomalous condition does not degrade further.

Ceiling and Visibility Launch Commit Criteria

The Shuttle ceiling and visibility launch commit criteria was evaluated in an effort to understand how the criteria were established and whether they needed to be updated. The evaluation focused on part of the launch commit criteria that states that, for short duration launch windows, the cloud ceiling at the pad can be no less than 6,000 feet for a cloud deck greater than 500 feet thick. The Shuttle Range Safety Panel requested this evaluation to determine if the launch commit criteria could be lowered to 5,000 feet to be consistent with the “Return to Launch Site” launch commit criteria ceiling limit.

The impact of lowering the ceiling launch commit criteria to 5,000 feet was measured by evaluating the casualty expectation (E_c). The study showed that with a constant delay time between vehicle failure and vehicle breakup, the overall risk remained constant with ceiling altitude. However, as the delay time between vehicle failure and vehicle breakup increased, the risk increased.

A delay time between 7 and 10 seconds resulted in acceptable E_c values; however, a delay time of approximately 15 seconds and above caused E_c violations. Traditionally, 7 seconds is the accepted delay time used for analysis. In the event that the Mission Flight Control Officers may need to initiate the Range Safety System, the lack of visibility of the vehicle due to a cloud ceiling would lessen the visual cues for the Mission Flight Control Officer and likely increase the delay time.

Space Shuttle Range Safety Panel

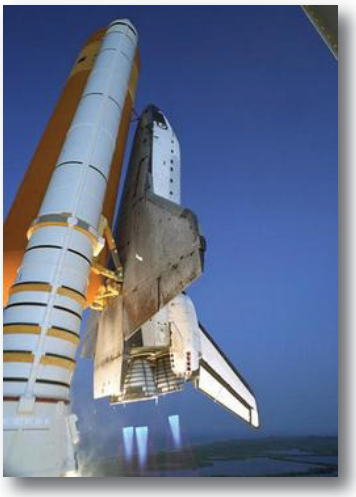
The Space Shuttle Range Safety Panel concluded that the cloud ceiling altitude did not significantly affect risk. Although lowering the launch commit criteria ceiling limit from 6,000 feet to 5,000 feet may yield acceptable risk values, the panel decided not to pursue the change at this time.

Command Receiver Decoder Implementation

The command receiver decoder replaced both the integrated receiver decoder and range safety distributor on the solid rocket booster range safety system and completed its first flight during the STS-118 mission in August 2007. The solid rocket booster range safety system, otherwise known as the airborne command destruct system, provides personnel and property protection in the event of flight path deviation or inadvertent vehicle breakup. The command receiver decoder was implemented due to supportability and obsolescence concerns for the integrated receiver decoder and range safety distributor previously used for all Shuttle missions.

Two command receiver decoders (System A and B) are required per solid rocket booster (four per flight). Their functions include providing control of the safe and arm device (System A only) in response to Orbiter master events controller or solid rocket booster multiplexer/demultiplexer commands and commanding the safe and arm device to SAFE during flight operations shortly before solid rocket booster separation. The command receiver decoder provides protection to the solid rocket booster retrieval crew by returning the safe and arm device to SAFE and turning off range safety power shortly before solid rocket booster separation.

In addition, the command receiver decoder provides isolation and interconnection for cross strapped ARM and FIRE commands between solid rocket boosters and ARM latching switch INHIBIT/RESET control. The command receiver decoder INHIBIT function protects the Space Transportion System and crew from inadvertent destruct during final launch countdown after ordnance is connected and the safe and arm device is commanded into the ARM position (T-4 minutes 55 seconds to T-10 seconds). The command receiver decoder also provides range safety system status to telemetry and ARMED indication to alert the crew.



The command receiver decoder routs range safety system measurements through the solid rocket booster multiplexer/demultiplexer to the Orbiter transmission system and provides energy output current pulse to fire the NASA standard detonator, initiating the pyro chain needed for airborne command destruct sequence. Before its first flight, the command receiver decoder was given exhaustive qualification testing to ensure compliance with revised loads environments. Additionally, an extensive flight safety review process ensured that the entire community was in agreement with the changes to the flight hardware and risk documentation.

Space Shuttle Range Safety Panel

Public Entry Risk Assessment Flight Rule Updates

Updates were made to Shuttle Flight Rule A2-207 to address the entry public risk consideration per the NPR 8715.5, *Range Safety Program*. The updates were a result of updated population numbers using LandScan 2005 and an updated probabilistic risk assessment incorporating late inspection to lower the overall probability of loss of vehicle. As a result of these analyses, it was seen that the current flight rule placards for nominal End-Of-Mission and Compromised Orbiter entries needed to be adjusted. The new flight rule was accepted during a Shuttle Flight Rule Control Board meeting in November 2007.